

PathGetShortPath

The destination string buffer must be long enough to hold the return file path

Sean Barnum, Cigital, Inc. [vita¹]

Copyright © 2007 Cigital, Inc.

2007-04-02

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 3876 bytes

Attack Category	<ul style="list-style-type: none">Malicious InputPath spoofing or confusion problem		
Vulnerability Category	<ul style="list-style-type: none">Buffer OverflowUnconditional		
Software Context	<ul style="list-style-type: none">File Path Management		
Location	<ul style="list-style-type: none">shellobj.h		
Description	<p>The in/out destination string buffer of function PathGetShortPath() must be long enough to hold an expanded file path.</p> <p>The PathGetShortPath() modifies the path parameter, in place, to find the "shortest path name" for the long path specified. A short path is usually defined in 8.3 standards. However, since the input path might be relative, it is possible for the resulting path to be longer than the input path. Therefore, the path variable should be at least MAX_PATH characters in length.</p> <p>This routine is part of a deprecated shellobj.h module that can be replaced with GetShortPathName.</p>		
APIs	Function Name		Comments
	PathGetShortPath		
Method of Attack	<p>This routine modifies a path parameter IN PLACE to convert it to a short path name (8.3 format). However, it is not guaranteed to be shorter than the original path due to relative path expansion. Therefore, the path buffer must provide extra space for expansion. Otherwise, an attacker might be able to provide a path name that expands and overflows the buffer.</p>		
Exception Criteria			
Solutions	Solution Applicability	Solution Description	Solution Efficacy

1. <http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html> (Barnum, Sean)

	<table><tr><td>Whenever PathGetShortPath is used.</td><td>The parameter, pszLongPath, must be at least MAX_PATH characters in length. Consider replacing with GetShortPathName which takes separate in and out buffers.</td><td>Effective.</td></tr></table>	Whenever PathGetShortPath is used.	The parameter, pszLongPath, must be at least MAX_PATH characters in length. Consider replacing with GetShortPathName which takes separate in and out buffers.	Effective.
Whenever PathGetShortPath is used.	The parameter, pszLongPath, must be at least MAX_PATH characters in length. Consider replacing with GetShortPathName which takes separate in and out buffers.	Effective.		
Signature Details	void PathGetShortPath(LPWSTR pszLongPath);			
Examples of Incorrect Code	<pre>WCHAR path[] = L"\\.\\AShort\\Path"; // Note: buffer is too small LPWSTR pszLongPath = path; PathGetShortPath(path);</pre>			
Examples of Corrected Code	<pre>WCHAR path[MAX_PATH] = L"\\.\\AShort\\Path"; // Note: buffer is correctly sized LPWSTR pszLongPath = path; PathGetShortPath(path);</pre>			
Source Reference	<ul style="list-style-type: none">http://msdn.microsoft.com/library/default.asp?url=/library/en-us/shellcc/platform/shell/reference/functions/pathgetshortpath.asp²			
Recommended Resource				
Discriminant Set	Operating System	<ul style="list-style-type: none">Windows		
	Languages	<ul style="list-style-type: none">CC++		

Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005-2007. Cigital retains copyrights to this material.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about “Fair Use,” contact Cigital at copyright@cigital.com¹.

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

1. <mailto:copyright@cigital.com>